HEADQURATERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400, APO AE 09131

DIRECTIVE
NUMBER 100-1

12 June 2002

# COMMUNICATIONS

## USEUCOM Policy for Management and Protection of Theater Communications Networks

1. **Summary**. This directive establishes U.S. European Command (USEUCOM) policy and prescribes responsibilities for operation and oversight of Theater common user networks, except for Extra High Frequency (EHF) Networks.

2. **Applicability**. This directive applies to all USEUCOM directorates/staff offices, components, and associated agencies operating in the USEUCOM area of responsibility (AOR).

3. **Internal Control Systems**. This directive contains internal control provisions and is subject to the requirements of the Internal Management Control Program. For HQ USEUCOM and subordinate joint activities, the applicable internal control directive is ED 50-8, Internal Management Control Program.

4. **Suggested Improvements**. Address suggested improvements to: HQ USEUCOM, ATTN: ECJ6-S, Unit 30400, APO AE 09131.

5. **References**. See Appendix A.

6. **Network Minimize Procedures**. See Appendix B.

7. **Policy**.

a. General.

(1) The USEUCOM Theater Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Coordination Center (TCCC) is the primary focal point for theater network visibility, deconfliction of theater network resources, and significant issues related to the operational health and security of network systems and services. The TCCC is the CINC's main network operations (NETOPS) center. It is the tool to ensure the C4ISR network satisfies mission requirements and functions effectively as a weapons system.

(2) Component NETOPS centers will provide the TCCC with timely and accurate information to ensure the CINC is provided the best possible information concerning the status of critical networks. This will consist of timely outage reports, network security status, significant upcoming network events, newly identified problems, positive and negative network trends and any other information deemed important.

b. Connection to USEUCOM's Theater Networks.

(1) All connections to the Defense Information System Network (DISN) require DISA-EUR technical approval after requirement validation by the appropriate authority; see reference A in Appendix A. Components have validation authority for circuits within their internal networks.

(2) The Joint Staff will validate all connections to the DISN by non-DOD, allied, or foreign agencies and activities prior to connection. These requests must be submitted to the TCCC for processing. See references B and C.

(3) Changes to the configuration of the DISN infrastructure (backbone) will be proposed to the appropriate Theater Configuration Control Board (TCCB) for approval prior to implementation. See reference D.

(4) Host Nation Approval (HNA) and Connection Approval (CA) are required before new communications equipment can be activated. Components are responsible for obtaining HNA from the individual countries. Per reference E, components must request CA through DISA.

(5) All connections to USEUCOM's military Defense Satellite Communications System require a Satellite Access Request (SAR) or Gateway Access Request (GAR) submission to ECJ6-O with a copy furnished to the DISA-EUR /Regional SATCOM Support Center (RSSC) Satellite Customer Service Center. SARs and GARs must go through individual components before coming to EUCOM for validation. Requests for commercial satellite bandwidth use the DoD Telecommunications Service Request/Telecommunications Service Order process, which will also require ECJ6-O validation prior to acquisition. Components have responsibility to validate Satellite Access Requests (SAR) with approved requirement from the SATCOM Data Base (SDB) prior to submission to ECJ6-O. Components must ensure that SDBs are up to date at their level prior to submission to EUCOM. See references M and N.

(6) Network Interconnection. The interconnection of networks under the security cognizance of different DAAs shall be documented and interconnected IAW reference L.

c. Use of USEUCOM Networks.

(1) USEUCOM's networks are to be used for official business and authorized purposes only. Using these services constitutes consent to have communications monitored for security and management purposes. If USEUCOM's networks become heavily congested, ECJ6 may instruct components through the TCCC to implement Minimize Procedures on theater data networks, (see Appendix B).

(2) Using USEUCOM networks to support Health, Morale and Welfare (HMW) is encouraged as an important means of enhancing morale. Components will implement procedures to ensure HMW uses of DISN do not compromise security, add significant cost or hamper official business.

d. Encryption/Network Defense. Encryption and network defense shall be implemented IAW ED 25-5 (see Reference L).

e. Information Operations (IO).

(1) The importance of information operations in the USEUCOM AOR extends far beyond military operations. IO encompasses actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending friendly information from hostile forces.

(2) Information operations are both defensive and offensive with overlapping areas. The Director of Operations, ECJ3, is responsible for all offensive IO while the Director C3 Systems, ECJ6, is responsible for defensive IO. A common link between the two aspects is the target sets involved. The Joint Staff continues to provide guidance on IO (see reference G).

(3) The Director C3 Systems, ECJ6, will provide an Information Warfare Defensive officer, who will also be a member of the standing USEUCOM IO Cell.

f. Spectrum Management.

(1) No commercial or military Communications-Electronics equipment will be introduced into the USEUCOM AOR until Host Nation Frequency Supportability is obtained and the equipment is determined to be compatible with the electromagnetic environment. Program managers and component forces must establish appropriate timelines, as this process is lengthy and takes 18-36 months, depending upon the Host Nation involved. Host Nation approval comments are required before application for operating frequency(ies) can be submitted by the appropriate component or office IAW reference H. Host Nation approval is not guaranteed.

(2) By law, no device that radiates or emits radio frequency energy is permitted to support military operations within the USEUCOM AOR without properly approved frequency clearances from the Host Nation which are obtained IAW reference H.

(3) For other than contingency operations, approval for military operating frequencies is also a lengthy process requiring Host Nation coordination. Commercial satellite frequencies must be coordinated, leased and funded by the program manager IAW commercial contracting procedures through appropriate embassies or Defense Attaches Offices (see reference I).

(4) The USEUCOM Spectrum Management Division (ECJ6-F) represents the DoD and USEUCOM concerning spectrum issues in NATO and international fora by providing the U.S. representative and assistant military representative to the NATO Frequency Management Subcommittee of the NATO C3 Board.

(5) The Spectrum Management Division will develop and publish the USEUCOM Spectrum Management Manual. This publication is directive in nature and based upon DOD and

Host Nation directives and agreements and provides procedural guidance for obtaining frequencies in the USEUCOM AOR.

(6) Frequency assignment records are owned and maintained by the component or organization that a) requested the frequency and owns the equipment (tactical) or b) installs operates and modifies equipment (strategic) (see reference H).

(7) The TCCC, in conjunction with the DISA/RSSC Satellite Customer Service Center, is the theater focal point for military and commercial band satellite access. The TCCC will review and validate all requests for military and commercial satellite access, which will consist of cross-referencing existing channel availability, checking customer priority, and getting final ECJ3 approval for access.

g. Information Management.

(1) Chief Information Officer (CIO). The Director, C3 Systems, is designated the USEUCOM CIO. The USEUCOM CIO's goals are to control C4I infrastructure and applications while influencing business applications to support the Warfighter. The USEUCOM CIO provides direct Warfighter input to the DoD CIO by influencing DoD process reengineering and participating in OSD policy and resource decisions.

(2) The USEUCOM CIO uses the Component CIOs to gain consensus on C4I issues and presents a consolidated Theater status and position to the Joint Community CIO (the Joint Staff J6) and the DoD CIO (ASD C3I) (see reference J).

8. Responsibilities:

a. HQs USEUCOM: The Director, Command, Control, and Communications Directorate, ECJ6, supervises the European segment of the Global Information Grid (GIG) and is responsible for establishing policy, restoration priorities, developing and validating system architectures, connection, and access requirements for any application or system using the electromagnetic spectrum and/or requiring long haul common-user information transfer services within USEUCOM. JWICS validations will be coordinated with J2. In addition ECJ6 will:

(1) Utilize the TCCC as the main focal point for all NETOPS activities to include network visibility, deconfliction of theater network resources, and any significant issues related to the operational health of network systems and services.

(2) Forward requirements requiring JCS approval as appropriate.

(3) Review service restoration priority requests in accordance with National Security and Emergency Preparedness (NS/EP) and Telecommunications Service Priority (TSP) procedures.

(4) Maintain a common operational picture of all critical USEUCOM networks through the TCCC.

(5) USEUCOM Inspector General, ECIG, will ensure Inspector General team surveys and reports include analysis of user telecommunications economy and discipline.

(6) Participate in all DISN-E configuration control and configuration management boards where policy and DISN-E way ahead issues are determined.

b. Defense Information Systems Agency (DISA). DISA defines the security, technical, interoperability, and performance standards for the entire DISN. DISA-EUR, as the field operating agency for DISA in the USEUCOM AOR, serves as the theater single system network manager of the DISN. DISA-EUR responsibility includes network monitoring and control of theater-wide DISN access points, DISN networks and backbone services. The DISA/RSSC Satellite One Stop Shop will be the theater focal point for EHF, UHF, and SHF satellite access. In addition DISA-EUR will:

(1) Provide the TCCC with timely and accurate information to ensure the CINC is provided the best possible information concerning the status of critical networks. This will consist of timely outage reports, significant upcoming network events, newly identified problems, negative network trends, and any other information deemed important.

(2) Approve all security, technical, and interoperability specifications for applications requiring DISN long-haul common-user information transfer services.

(3) Establish procedures for and chair the DISN-Europe configuration management board and the theater Configuration Control Boards (CCB) for voice, data, and transmission systems. Procedures will include board composition, meeting frequency and method.

(4) Provide operational management of the DISN and implement solutions.

(5) When requested by USEUCOM provide a full time liaison officer to augment the TCCC operations.

c. Other. USEUCOM component commands, DOD agencies, services and their elements operating in the USEUCOM Theater are responsible for efficient operations, maintenance, and funding of the deployed block and designated portions of the sustaining block of the DISN such as user data terminal equipment, telephones, facsimile machines, computers, video teleconference suites, premise routers, base outside plant, firewalls etc. They are responsible for ensuring that their portions of the DISN conform to security, technical, interoperability, and performance standards established by DISA. In addition they will:

(1) Provide the TCCC with timely and accurate information to ensure the CINC is provided the best possible information concerning the status of critical networks. This will

consist of timely outage reports, significant upcoming network events, newly identified problems, negative network trends, and any other information deemed important.

(2) Ensure all necessary Host Nation Approvals and Connection Approvals have been obtained prior to fielding systems in this theater.

(3) Ensure that internet protocol (IP) capable systems use NIPRNET and SIPRNET, or JWICS services unless waivered. Interoperability, timeliness of services, and network integrity/control, combined with enterprise-level cost optimization, shall form the basis for the waiver process.

(4) Obtain electromagnetic spectrum approval and validation of DISN access before connecting to theater networks.

(5) Components will establish audit procedures for DISN-provided services and review requirements on a biennial basis.

(6) Validate access and connection requirements for applications and systems at the individual local base, post, camp, or station.

(7) Components' headquarters shall validate all urgent telecommunications requirements with DISA-EUR prior to submission of an urgent Request for Service (RFS). Validation for urgent RFSs at component headquarters must be accomplished at the O-6/GS civilian equivalent level.

(8) When requested by USEUCOM, provide a full-time liaison officer to augment the TCCC operations.

(9) Participate in all DISN-E configuration control and configuration management boards.

9. Summary of Changes. This directive:

a. Replaces ED 100-1 (Defensive Information Warfare IW-D), ED 100-2 (Emergency Evacuation/Destruction of Defense Information Infrastructure Sites, 10 Feb 2000), ED 100-6 (Management and Use of the Electromagnetic Spectrum, 10 Apr 2000), ED 100-8 (Theater Policy for the Defense Information Systems Network, 26 Mar 98). ED 55-10 Technical Interface Guide (TIG), 13 Apr 2000, will be converted to USEUCOM Pamphlet 100-1. Additionally ED 100-3 is cancelled. Information is now contained in the MILSTAR CEOI.

b. Incorporates USEUCOM specific policy and guidance for the management of USEUCOM networks into a single policy document.

c. Implements policy for the TCCC to exercise oversight of theater networks.

d. Establishes the requirement for HNA and CA to be obtained before equipment is nominated as a technical solution to fill a requirement.

e. Establishes the DISN as the primary DoD long-haul command and control for telecommunications networks within USEUCOM.

f. Incorporates DISA-EUR policy for configuration management of the DISN.

g. Establishes policy and responsibilities for DISN management, use, and access.

h. Establishes procedures for limiting traffic on USEUCOM's data networks.

FOR THE COMMANDER IN CHIEF:

OFFICIAL:

DANIEL J. PETROSKY
Lieutenant General, USA
Chief of Staff

AVA N. WEBB-SHARPLESS
Lt Col, USAF
Adjutant General

APPENDIXES:

A - References
B - Minimize Procedures

DISTRIBUTION:
P

## APPENDIX A

### References

a. DISA Circular 310-130-1, 4 Apr 2000 and DISA-EUR Sup 1, Submission of Telecommunications Requests.

b. CJCSI 6211.02A, 22 May 96, Defense Information System Network and Connected Systems.

c. CJCSI 6740.01, 1 Sep 96, Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations.

d. DISAEI 300-50-1, 15 Apr 98, DISA-Europe Policy for Implementing Configuration Management within the Defense Information System Network-Europe (DISN-E).

e. DISA-EUR-Circular 310-140-2, Leased Services and Facilities Connection Approval Procedures.

f. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 DEC 97.

g. CJCSI 6510.01A, Defensive Information Warfare, 30 Nov 99.

h. USEUCOM Spectrum Management Manual (SMM) Volume 1, Feb 98.

i. USEUCOM Directive 56-9, 23 June 98, European Command Relationships and U.S. Defense Representatives.

j. CJCSI 8010.01, Joint Community Chief Information Officer.

k. CJCSI 6510.01C, Information Assurance and Computer Network Defense, 1 May 2001.

l. USEUCOM Directive 25-5, Information Assurance, 12 Apr 2002.

m. CJCSI 6250.01A, Satellite Communications, 10 Dec 2001.

n. USEUCOM Pamphlet 100-1, Technical Interface Guide, 13 Apr 2000.

## APPENDIX B

### Defense Information System Network-Europe
### Minimize Procedures

**1. Purpose.** The purpose of this policy is to outline procedures to conserve bandwidth on the DISN during mission critical periods.

**2. Applicability.** This policy is applicable to all personnel within the USEUCOM Theater who use DISN services.

**3. General.** The DISN provides U.S. warfighters with the ability to send and receive vital information quickly and efficiently. During contingency operations, DISN services can be adversely affected due to excessive demand. During these periods, vital command and control communications can be jeopardized due to congestion. When conditions warrant, the ECJ6 may impose minimizing procedures on non-essential NIPRNET and SIPRNET use. In such cases, components will comply by implementing the following limitations:

a. Level I Minimize.

(1) E-mail, Voice Calls, and VTC: Limit E-mail, voice calls and VTC sessions to mission-essential traffic only and morale support on a non-interfering basis, (i.e., no personal e-mail, phone calls, or VTCs unless morale support is command-directed on a non-interfering basis). Use of the return-receipt feature will be prohibited except for mission critical command and control where positive acknowledgement is required. Use of the "Reply" and "Reply To All" feature will be limited to the maximum extent possible. Limit courtesy copy addresses ("cc") to those with a genuine need to know. Eliminate unnecessary/excessive graphics in presentation files.

(2) Web Usage: Download large files from web sites only when mission essential.

(3) Web Sites: Post large file attachments to web sites rather than sending to numerous individuals through e-mail.

b. Level II Minimize (these actions will be in addition to level I):

(1) E-mail: Limit the size of E-mail attachments to less than 10mb. Use file compression utilities when sending files.

(2) Web Usage: Use of “.com” web sites will only be allowed in support of military applications dependent on interaction with the internet.

(3) Internet Protocol (IP) VTC: IP-based voice and video teleconferencing will be prohibited.

(4) Collaborative Planning Tools: Use of collaborative planning tools will be limited to those which are mission essential. Video teleconferencing option will be disabled.

4. USEUCOM will direct components to impose Levels I or II minimize when the DISN backbone is reaching dangerous levels of congestion. Components are free to impose some or all of these procedures at any time they are experiencing congestion on their internal networks.

5. If imposition of these minimizing procedures fails to reduce congestion on the DISN, ECJ6 will instruct DISA-EUR to identify additional actions which could be taken to preserve the integrity of the backbone.